Einiges aus der Kryptographie (Zusammenfassung)

Henze, Ernst

Veröffentlicht in:
Jahrbuch 1985 der Braunschweigischen Wissenschaftlichen Gesellschaft, S.15

Verlag Erich Goltze KG, Göttingen

8.2.1985 in Braunschweig

Einiges aus der Kryptographie

(Zusammenfassung)

Von **Ernst Henze**

Ausgehend von einem historischen Überblick wird das allgemeine Problem des Chiffrierens, d.h. der Geheimschriften mathematisch erläutert. Verschiedene, der Art nach unterschiedliche Verfahren werden geschildert und die allgemeine Problemstellung sowie die allgemeine Lösung aufgeführt. Diese Lösung ist natürlich in der Regel nur approximativ zu erreichen. Nach einem Überblick, auch über einige elektronische Verfahren, wird ein kurzer Abriß der modernen Theorie der Bibliotheks-Schlüsselverfahren gegeben. Für diese wird eine allgemeine Funktionalgleichung für die sogenannten Einweg-Funktionen abgeleitet und einer geschlossenen Lösung zugeführt.

Die Arbeit erscheint in leicht geänderter Form in den mathematischen Semesterberichten 1986.